AZ-500: Microsoft Azure Security Technologies

Microsoft - Azure Apps & Infrastructure

Live Training (também disponível em presencial)

- **Localidade:** Porto
- **Data:** 11 Dec 2023
- **Preço:** 1590 € (Os valores apresentados não incluem IVA. Oferta de IVA a particulares e estudantes.)
- **Horário:** Laboral das 09h00 - 17h00
- **Nível:** Intermédio
- **Duração:** 28h

Sobre o curso

This course provides IT Security Professionals with the knowledge and skills needed to implement security controls, maintain an organization's security posture, and identify and remediate security vulnerabilities.

This course includes security for identity and access, platform protection, data and applications, and security operations.

Destinatários

- This course is for Azure Security Engineers who are planning to take the associated certification exam, or who are performing security tasks in their day-to-day job. This course would also be helpful to an engineer that wants to specialize in providing security for Azure-based digital platforms and play an integral role in protecting an organization's data.

Pré-requisitos

Successful learners will have prior knowledge and understanding of:

- Security best practices and industry security requirements such as defense in depth, least privileged access, role-based access control, multi-factor authentication, shared responsibility, and zero trust

model.
- Be familiar with security protocols such as Virtual Private Networks (VPN), Internet Security Protocol (IPSec), Secure Socket Layer (SSL), disk and data encryption methods.
- Have some experience deploying Azure workloads. This course does not cover the basics of Azure administration, instead the course content builds on that knowledge by adding security specific information.
- Have experience with Windows and Linux operating systems and scripting languages. Course labs may use PowerShell and the CLI.

Programa

- Manage identities in Microsoft Entra ID
- Manage authentication by using Microsoft Entra ID
- Manage authorization by using Microsoft Entra ID
- Manage application access in Microsoft Entra ID
- Plan and implement security for virtual networks
- Plan and implement security for private access to Azure resources
- Plan and implement security for public access to Azure resources
- Plan and implement advanced security for compute
- Plan and implement security for storage
- Plan and implement security for Azure SQL Database and Azure SQL Managed Instance
- Plan, implement, and manage governance for security
- Manage security posture by using Microsoft Defender for Cloud
- Configure and manage threat protection by using Microsoft Defender for Cloud
- Configure and manage security monitoring and automation solutions

Manage identities in Microsoft Entra ID

- Enhance security in Microsoft Entra ID to safeguard user identities and accounts.
- Implement security for group management in Microsoft Entra ID for effective access control.
- Advise on the secure management of external identities in Microsoft Entra ID.
- Utilize Microsoft Entra ID Protection for proactive threat detection and response.

Manage authentication by using Microsoft Entra ID

- Set up Microsoft Entra Verified ID for trusted identity verification.
- Implement multifactor and passwordless authentication for enhanced security and convenience.
- Enforce password protection measures and single sign-on for simplified, secure access.
- Integrate SSO with identity providers and endorse modern authentication protocols.

Manage authorization by using Microsoft Entra ID

- Set Azure role permissions across management groups, subscriptions, and resources for access control.
- Assign built-in roles in Microsoft Entra ID and Azure for predefined user permissions.
- Create custom roles in Azure and Microsoft Entra ID to match organizational access needs.
- Manage Entra Permissions, Privileged Identity Management, and Conditional Access for refined control and compliance.

Manage application access in Microsoft Entra ID

- Manage enterprise application access in Microsoft Entra ID, including OAuth permission grants for access control.
- Govern application integration with identity platforms through Microsoft Entra ID app registrations.
- Configure app registration permission scopes for appropriate resource access levels.
- Manage app registration consent and use service principals and managed identities for automated management and enhanced security.

Plan and implement security for virtual networks

- Implement security measures for Azure virtual networks to safeguard data and resources.
- Utilize NSGs and ASGs for network traffic security, and manage UDRs for optimal traffic routing.
- Establish secure network connectivity through Virtual Network peering, VPN gateways, and Virtual WAN.
- Enhance network security with VPN configurations, ExpressRoute encryption, PaaS firewall settings, and Network Watcher monitoring

Plan and implement security for private access to Azure resources

- Develop security strategies for private access to Azure resources to protect sensitive data.
- Utilize virtual network Service Endpoints and Private Endpoints for secure Azure service access.
- Manage Private Link services for secure resource exposure and integrate Azure App Service and Functions with virtual networks.
- Configure network security for App Service Environment and Azure SQL Managed Instance to safeguard web applications and databases.

Plan and implement security for public access to Azure resources

- Develop strategies for secure public access to Azure resources, preventing unauthorized access and breaches.
- Implement TLS for Azure App Service and API Management to encrypt data in transit.
- Protect network traffic with Azure Firewall and Application Gateway for optimized web application security and delivery.

- Enhance web app performance with Azure Front Door and CDN, and deploy WAF and DDoS Protection for robust defense against attacks.

Plan and implement advanced security for compute

- Enhance Azure compute resources' security against vulnerabilities and attacks with advanced measures.
- Secure remote access via Azure Bastion and JIT VM access, and implement network isolation for AKS.
- Strengthen AKS clusters' security, monitor Azure Container Instances and Apps, and manage access to Azure Container Registry.
- Implement disk encryption methods like ADE and manage API access securely in Azure API Management.

Plan and implement security for storage

- Develop security strategies for Azure storage resources, ensuring data protection during rest and transit.
- Manage storage account access with effective access control and secure key lifecycle management.
- Tailor access methods for Azure Files, Blob Storage, Tables, and Queues to specific use cases.
- Strengthen data security with soft delete, backups, versioning, immutable storage, BYOK, and double encryption.

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Implement security for Azure SQL Database and Managed Instance to safeguard sensitive data.
- Use Microsoft Enterprise Identity for database authentication and conduct database auditing for compliance.
- Utilize Microsoft Purview for data governance and classification to protect sensitive information.
- Apply dynamic masking and Transparent Database Encryption, and recommend Always Encrypted for client-side data protection.

Plan, implement, and manage governance for security

- Enforce compliance using Azure Policy to create and manage security policies.
- Streamline secure infrastructure deployment with Azure Blueprint.
- Utilize landing zones for consistent Azure security and manage sensitive data with Azure Key Vault.
- Enhance key security with HSM recommendations, effective access control, and regular key rotation and backup processes.

Manage security posture by using Microsoft Defender for Cloud

- Utilize Microsoft Defender for Cloud Secure Score and Inventory to identify and mitigate security risks, enhancing overall security posture.

- Assess and align with security frameworks using Microsoft Defender for Cloud to ensure adherence to security standards and best practices.
- Integrate specific industry and regulatory standards into Microsoft Defender for Cloud for tailored compliance.
- Connect hybrid and multicloud environments to Microsoft Defender for Cloud for centralized security management, and monitor external assets to safeguard against external threats.

Configure and manage threat protection by using Microsoft Defender for Cloud

- Utilize Azure Monitor for comprehensive monitoring of cloud security events.
- Aggregate diverse security data efficiently with data connectors in Microsoft Sentinel.
- Detect threats using customized analytics rules in Microsoft Sentinel.
- Assess and automate incident responses in Microsoft Sentinel for enhanced security management.

Configure and manage security monitoring and automation solutions

- Use Azure Monitor for effective security event monitoring in cloud environments.
- Implement data connectors in Microsoft Sentinel for comprehensive security data collection.
- Develop customized analytics rules in Microsoft Sentinel for targeted threat detection.
- Assess and automate responses to security incidents in Microsoft Sentinel to enhance workflow efficiency.